# Network Security Issues in The Internet of Things (IoT)

Stuart Millar, *PhD Cyber Security Student, 13616005, Queen's University of Belfast*

***Abstract*— This paper surveys a broad range of other research works in order to discuss network security issues in the Internet of Things (IoT). We begin with setting the scene generally with an outline of IoT, followed by a discussion of IoT layer models and topologies. After this, IoT standardization efforts and protocols are analysed, before we discuss in depth vulnerabilities, attacks and mitigations with regard IoT. It is concluded that ample research and narrative exists for protocols and vulnerabilities but less on mitigations, particularly with regard Intrusion Detection Systems (IDS) for IoT, and resource constraints on devices are a considerable obstacle in strengthening security.**

***Index Terms*—counter-measures, internet of things, mesh networks, mitigations, network security, security, sensors, vulnerabilities.**

## I. Introduction

The term 'Internet Of Things' (IoT) was created by Kevin Ashton in 1999 and then formally introduced by the International Telecommunication Union (ITU) in the ITU Internet report in 2005. The Cluster of European Research Projects (CERP) defines IoT as allowing people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. 'Things' are actual objects, for example wearables, thermostats like Google Nest, sensors in a car to detect speed or lighting sensors [1].

IoT connects these objects together, letting them access the cloud, transfer data and provide information. Things can be controlled remotely and also act as a gateway to the internet. By 2020 it is estimated that 4.5 billion new people and 37 billion new things will have joined the internet [2]. The term Network of Things (NoT) will also be used in this paper, and we can say the IoT is made up of various NoT.

IoT devices will have access to our sensitive personal data – as per the HP IoT Research study [3], suddenly everything from fridges to sprinklers are wired and interconnected, which creates new attack opportunities for hackers. HP analysed devices from manufacturers of TVs, webcams, thermostats, door locks, home alarms, and more, finding some interesting results – 70% of devices used unencrypted network services and the majority failed to encrypt network services transmitting data via the internet and the local network.

This paper was submitted on 21st October 2016 by Stuart Millar, PhD Cyber Security student at the Queen's University of Belfast. Student number 13616005. Email: smillar09@qub.ac.uk

Indeed, HP say that users are one network misconfiguration away from exposing this data to the world via wireless networks. Leo, Battisti, Carli and Neri [4] state that the wide spread of sensors and actuators will increase the exposure of objects to cyber attacks. This is true of NoT present at home, in the office, and also in Industrial Control Systems (ICS) - the Stuxnet malware worm, which caused massive disruption to Iranian nuclear centrifuges, is an example of NoT being compromised and ICS being damaged. In fact, in the US the National Cybersecurity and Communications Integration Center (NCCIC) has a specialist ICS team that reports on such incidents, showing its importance [4].

## II. An outline of IoT

To begin with, the early work of Karlof & Wagner back in 2003 [5] concerned secure routing in IoT, attacks and countermeasures. This is something of a seminal paper. They compare IoT with more traditional wireless networks, noting the resource constraints in IoT. Sensor nodes have slow processors, limited computational power and little memory storage, typically comprising an 8-bit processor, RAM measured in KB rather than MB, a small radio and tiny battery. Shang, Yu, Droms and Zhang [6] give more detail on the power constraints, explaining IoT networks often use low-energy technologies such as IEEE 802.15.4, Bluetooth and low-power Wi-Fi. These usually operate with a smaller Maximum Transmission Unit (MTU) and lower transmission rate than normal Ethernet links. So packet sizes in IoT have to be smaller, and hence already we encounter a key technical challenge in keeping messages and packet overheads low. Garcia-Morchon et al [7] also point out IoT resource constraints cause reliance on lossy and low-bandwith channels, with resource expensive cryptography limited too.

Kim, Wasicek, Mehne and Lee [8] present a realistic view that NoT will be deployed in open, physically insecure or hostile environments open to attack. [5] significantly describes some attacks for the first time, like the *sinkhole attack*, the *HELLO flood*, the *wormhole attack* and the *Sybil attack*. We shall discuss these vulnerabilities and more, plus countermeasures and mitigations, later in this paper.

[5] introduces the idea of NoT having points of centralised control called base stations, which are gateways to another network, data storage / processing centres or an access point for a human interface. Traditional networks are point-to-point, or end to-end, whereas NoT traffic can be many-to-one (sending

data from nodes to a base), one-to-many (base to nodes communication, like a multicast or a message flood) and local (for example neighboring nodes talking). Roman and Lopez [9] raise the idea, on the other hand, of decentralizing, where all nodes participate in decision making and internal protocol, known as a flat configuration, or dividing NoT into clusters of nodes, each with a cluster head to make decisions, known as a hierarchical configuration.

Nalbandian [1] gives a suitable outline of IoT, though lacks detail one expects with regard specific security challenges, for example mentioning Radio Frequency Identification (RFID) usage without mentioning its vulnerabilities, though these are presented by Xingmei, Jing and He [10], which we will review. However, other papers do address specific security challenges. [1] points out the simple lack of human control means the devices need managed and protected, a moot point really. [1] could have been improved with more information on topologies and implementation details, which we will discuss by gathering points from [9], Zegzhda and Stepanova [11] and [7].

## III. IoT Layer Models

To help understand IoT compared to traditional networks, two different layer models are proposed by previous research, in a similar fashion to the well-known OSI model for networking. Firstly, Mahoud, Yousuf, Aloul and Zualkerman [12] present a simple model of three layers - *perception*, *network* and *application*. This is perhaps a little basic given the complexity of IoT, and the paper does not compare it with the second model that CISCO [2] have proposed.

The three-layer model consists of:

*1) Perception layer* – consider this a sensor layer, acquiring data from an environment via sensors and actuators. This layer detects, collects and processes info before transmitting it to the network layer.
*2) Network layer* – performs IoT node collaborations in local and short range networks. Handles data routing and transmission to different IoT hubs and devices over the internet. Clouds, gateways, switches and routers use wireless protocols here.
*3) Application layer* – guarantees authenticity / integrity / confidentiality of data.

CISCO contend that IoT-ready networks need a different communication and processing model. As it stands today, there is not a standard way of understanding or describing these models. CISCO offer an IoT reference model of seven layers (see figure A). Their model aims to help secure each device or system, provide security for all processes at each level, plus secure movement and communications between each level, whether north bound or south bound:

*Layer 7 – Collaboration and Processes* - involving people and business processes, e.g. identity management software.
*Layer 6 – Application* – involves reporting, analytics and control e.g. authentication/authorization software.
*Layer 5 – Data Abstraction* – involves aggregation and access, and secure storage e.g. hardware and software solutions.
*Layer 4 – Data Accumulation* – also involves storage e.g. tamper resistant software.
*Layer 3 – Edge (Fog) Computing* - data element analysis and transformation where the network meets the cloud e.g. secure communications via protocols and encryption.
*Layer 2 – Connectivity* – involves communication and processing units e.g. secure network access via hardware and protocols.
*Layer 1 – Physical Devices and Controllers* – these are the things in IoT.

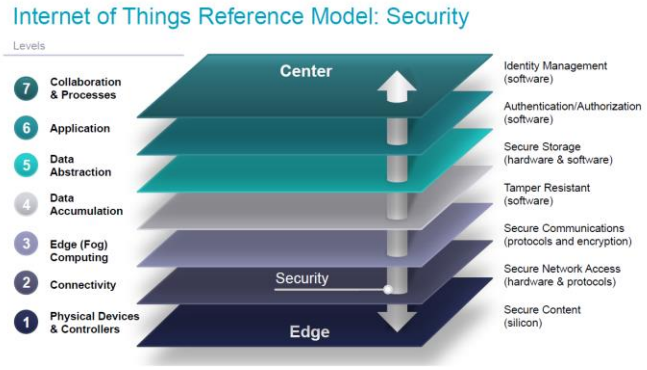


Fig. A. The CISCO seven-layer model [2].

Mohsen and Jha [13] also use the CISCO model to discuss IoT and mostly consider the edge side layers 2 and 3 above. We shall study the attacks contained in [13] later in this paper.

## IV. IoT Topologies

[11] proposes three useful topologies: *point to point*, *star* and *mesh*. The latter is decentralized, and preferable. Mesh has a gateway node, simple sensor nodes, and nodes that can work as both sensors and routers. [11] recommends decentralised mesh for mitigation, agreeing with [9] in saying centralization has a weakness in providing a single point of failure if using the front-end proxy solution. [7] also agrees, stating that using a central security manager represents a single point of failure and fixes network roles statically, with decentralized and distributed architecture being more dynamic. [6] contends that the fundamental challenge of routing in IoT mesh networks comes from the requirement of maintaining routing information for each host in a multilink environment. This is not an issue in traditional IP networks where routers or self-learning bridges can be deployed to provide infrastructural support for routing and forwarding. However, in constrained IoT environments, the per-host routes are either maintained by every node in the mesh using routing protocols, which consumes lots of memory, or carried with the IP packet as source routes during forwarding which conflicts with the small MTU restriction.

## V. IoT Standardisation & protocols

Convergence toward an IP-based communication stack is necessary as IoT has very diverse wireless communications with gateway devices needed for protocol translation. The surveyed papers discuss numerous protocols with 6LoWPAN, IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), Datagram Transport Layer Security (DTLS),

Constrained Application Protocol (CoAP), IPSec and Radio Frequency Identification (RFID) mentioned most.

Firstly, consider the large number of IP addresses required in the IoT. IPv4 cannot support this, so IPv6 will be used. However, with the device limitations additional protocols are needed. The Internet Engineering TaskForce (IETF) have developed 6LoWPAN and RPL. 6LoWPAN uses compression to allow IPv6 packets to be sent over wireless networks made up of resource constrained devices. CoAP is an application layer protocol to let devices communicate, using User Datagram Protocol (UDP). It can be translated to HTTP for use over the web. According to [7], DTLS is the basic building block for protecting CoAP. TinyDTLS is the first open-source implementation of the protocol for small devices but it has not really been road-tested. DTLS was designed for computer networks rather than IoT, and [6] points out DTLS imposes high overheads on IoT devices. The loss of a message in flight requires retransmitting all messages – far from ideal.

Elbouanani, Kiram and Achbarou [14] explain further how 6LoWPAN defines header compression to allow IPv6 packets to be sent between resource constrained devices and make the point that a common set of standards are needed for IoT. They also give more detail on the three RPL modes of varying levels of security (*unsecured, preinstalled and authenticated*) which other papers do not seem to do.

Keoh, Kumar and Tschofenig [15] note the optimisation of DTLS for CoAP, and that IETF are working on a standard way of granting permissions and authorizing IoT to accept each other's resources. They suggest two other protocols for security as well as DTLS – 1) IPSec, for channel security via AH (Authentication Headers) and data security via ESP (Encapsulating Security Payloads) traffic, and 2) IKEv2, which is used to establish IPSec. Interestingly [9] says IPSec is not supported for network layer security when using the 6LowPAN spec but is sparse on reasons why.

Fragmentation due to a smaller MTU is problematic and open to attack as mentioned in other papers such as [7]. The trend of identifying IPSec and DTLS continues in [7]. [6] and [15] develop the fragmentation and small MTU issues well, with the latter explaining at most 102 bytes are available for an IP packet after taking into consideration MAC frame header size and security. Of this 102, another 48 bytes are needed for IPv6 and UDP headers, leaving just 64 bytes for application data and its security protection. Hence fragmentation is needed, and as stated this is vulnerable.

[15] also references 6LoWPAN, RPL and CoAP for resource constrained devices and discusses standardisation in IoT, looking specifically at protocols to be used in conjunction with CoAP. According to [15], DTLS has been chosen as the channel security under CoAP for IoT. [15] says standardised security protocol is indispensable for success of IoT. DTLS was not designed for constrained environments though - it still has its weaknesses, as discussed in [7], with packet fragmentation and having to retransmit all messages in flight if one listed as drawbacks. [15] argues that a critical mass of devices may be needed to achieve an interoperable/standardised IoT, and designing a totally new protocol may seem like reinventing the wheel. However, as per the future device figures outlined initially in this survey paper, a critical mass of devices is inevitable.

RFID is common in IoT. RFID tags containing antennae are attached to objects so they can be tracked and identified via wireless/radio technology. However, it is vulnerable, as we will see, and work needs to be done for connecting RFID devices over the actual internet.

[14] introduces MQTT (formerly MQ Telemetry Transport) as another protocol not seen in other papers, which was created by OASIS. MQTT is simple and lightweight, again suiting resource constrained devices. Andrea, Chrysostomou and Hadjichristofi [16] also contend that MQTT, along with CoAP, is most commonly used in IoT.

## VI. IoT Vulnerabilities & attacks

In cyber security, the Confidentiality – Integrity – Availability (CIA) triad is well known. None of the surveyed papers however relate CIA back to IoT apart from [13]. The Open Web Application Security Project (OWASP) also have a useful list of IoT Attack Surface Areas which they state should be understood by manufacturers, developers, researchers and companies looking to deploy IoT in their organisations [17]. As mentioned, [5] outlined some IoT attacks for the first time and these are regularly referenced in the literature (for example by Wood, Fang and Stankovic [18], and [16]) – these are the *sinkhole attack*, the *Sybil attack*, the *wormhole attack*, the *HELLO flood* and *acknowledgement spoofing*:

*1) Sinkhole attack* – all traffic is lured from an area through a compromised node, where selective forwarding can follow with the attacker deciding what data to allow through.
*2) Sybil attack* – a single node presents multiple identities to others in the network, so an attacker can be in more than one place at once.
*3) Wormhole attack* – an attacker tunnels messages received in one part of the network over a low latency link and replays them in a different part.
*4) HELLO flood* – here the attacker causes every node to mark it as their parent. Most nodes will be out of range and this causes a lot of packets to be lost. Routing loops can be set up too via spoofing routing updates, with two nodes being attacked and redirecting packets to each other.
*5) Acknowledgement spoofing* - used for a selective forwarding attack, where an attacker strengthens/weakens networks links so packets are lost from a node.

[13] discusses the attacks at layer 2 and layer 1 of the CISCO seven-layer model, stating conventional network attacks are also applicable to IoT:

*Layer 2: Connectivity - attacks*

*a) Eavesdropping / sniffing* – gains usernames, passwords, node identifiers and other useful data.
*b) DoS attacks* – jam the transmission of radio signals or, via a malicious node, refuse to route messages, or redirects them where they shouldn't go.
*c) Injecting fraudulent packets* – done via insertion (where malicious packets that seem legit are generated and sent), manipulation (when packets are captured then modified) and

replication (where the attacker captures packets between two things to replay them).
*d) Routing attacks* – an attacker can spoof, redirect, misdirect or drop packets, for example the wormhole, HELLO flood and Sybil attacks.

*Layer 1: Physical devices & controllers - attacks*

*a) Denial of Service (DoS)* attacks – such as battery draining by an attacker sending lots of packets, outage attacks, or when an edge device stops performing its normal operation, like the Stuxnet attack mentioned in this paper's introduction.
*b) Node replication attacks* – the attacker adds a new node to an existing set by replicating another node's ID number. This can lead to reduction in network performance and the attacker can easily corrupt or misdirect packets that arrive at the replicated node.
*c) Camouflage* - the attacker inserts a counterfeit edge node or attacks an authorized node to hide at the edge level. Then it can obtain and manipulate packets, or be passive and just analyse traffic.

Gubbi, Buyya, Marusic and Palaniswami [19] make a valid point that RFID is a weak protocol that allows person tracking and object tracking. These devices are too small to use complex security algorithms. They suggest cryptography can help, air the idea of *digital forgetting* to protect privacy, and state new protocols are a large area of research. However, they do not delve into the specifics of attacks. The threats to RFID are significant, well summarised by [10]:

*1. Replication attack* – copy or forge identical RFID labels.
*2. Channel Blocking attacks* – channel is occupied for a long time and legit communications can't be transferred.
*3. Forgery attack* - legit RFID label is obtained by using special hardware facilities of counterfeit.
*4. Impersonation attack* – attacker fakes a legit reader to steal or change RFID tag info.
*5. Tampering attack* – attacker will modify the info and pass it on to receiver.

[13] adds to the RFID threats detailing:

*1. Tracking* – in close proximity a reader can read a tag. Dangerous when combined with personal info.
*2. Inventorying* – info can be deduced from device tags
*3. DoS* – RF channels are jammed so the tags cannot be read by tag readers and the intended services become unavailable, e.g. locking down a whole building.
*4. Eavesdropping* – messages are intercepted/read/saved for future.

Eavesdropping, routing attacks and DoS attacks are common themes in [7] too, with conventional Man-In-The-Middle (MITM) attacks also possible in IoT if keying material is exchanged in the clear, or if device authentication is non-trivial and needs human interaction. [12] discusses attacks in terms of its three-layer model similar to [13], specifically for a network layer – like [7], it points out it is susceptible to DoS attacks, MITM and eavesdropping though does lack the depth of info from other papers.

[8] notes that authentication based on digital certificates cannot scale to the size needed. This paper also recommends using DTLS and CoAP, though warns that DTLS is for point-to-point rather than publish-subscribe (i.e. one-to-many). [6] gives a warning for DTLS that other papers do not give, contending DTLS applies in IP-based apps but as a secure channel solution it does not fit into IoT for several reasons. Firstly, there is the overhead of establishing a channel, and secondly both ends of the channel having to maintain the state of the channel until it closes. This hinders memory usage when a device needs to communicate with many peers simultaneously in a densely-meshed network.

## VII. Mitigations / Counter Measures

A layered approach is always best - [9] says that IoT must be secured from hardware of nodes right through to applications, and the surveyed papers make recommendations for mitigation in different areas. Tankard [20] recommends a holistic view by designing security in from the operating system, using the devices hardware capabilities and extending up the device stack. This paper lacks detail, but rightly points out that adding security to legacy devices, rather than solely focusing on devices to come, is important. Other papers have failed to recognise legacy vulnerabilities to the same extent. [16] outlines that securing premises is perhaps the most important – this is a short-sighted point in truth. [15] and [7] say that the computational capabilities of embedded systems in IoT will improve and so eventually they will be able to run the full IP protocol stack, meaning some mitigations may be temporary. Still, we need to look at the present situation. Mitigations include:

### *A. Choice of Protocol:*

Specifically proposed in [7] as a countermeasure to DoS are DTLS and IPSec/IKEv2. They implement return route checks based on cookies to delay state establishment until the initiating host address is verified. [7] also suggests puzzle-based approaches that forces the initiator to solve cryptographic puzzles of varying difficulty. This should be used with care, as under attack conditions that reduce device performance, clients may not be able to solve these puzzles and suffer exclusion. [7] states DTLS together with IPSec/IKEv2 provide end-to-end security services including peer entity authentication, end-to-end encryption and integrity protection.

[18] proposes Secure Implicit Geographic Forwarding (SIGF), a configurable secure routing protocol for NoT. It does not use routing tables, preventing state corruption, wormholes and HELLO floods. Still, this protocol is open to DoS and Sybil attacks.

To reduce packet loss, [6] suggests legacy protocols should be redesigned to minimise use of IP multicast before they can be applied to IoT. They say is it better for nodes to pull packets on-demand from a store where packets are buffered. In addition, [13] offers depattern-ing as a mitigation, where fake packets are inserted to fool the attacker. This is a novel

idea and was not present in other papers that suggested mitigations.

[8] concludes that secure routing is vital to acceptance and use of IoT, though current routing protocols are insecure with a new standard being needed, and we should be aware of attacks coming from more powerful devices outside the network i.e. powerful laptops and desktops which can easily break cryptography.

### *B. Choice of Topology:*

[11] points out decentralised topology is good for mitigation and uses Wireless HART as an example. It does say the IoT evolution plateau will be circa 2025, but given the speed of progress, which could be considered exponential, this plateau could be sooner.

### *C. Consider Application Data Security:*

The IETF has suggested object-based security which secures the application data directly rather than securing the channel through which the data is transmitted [8]. Each object should have digital signatures so anyone receiving it can verify its validity.

### *D. Intrusion Detection Systems (IDS):*

Raza, Wallgren and Voigt [21] proposed an IoT specific IDS called SVELTE, with the driving force being that message security is of course an issue but nevertheless networks are vulnerable to a number of attacks to disrupt services. [13] references SVELTE as one of the first IDS for IoT, Gendreau and Moorman [22] seems to go so far as saying that the prevention of unauthorised access to IoT will depend on intrusion detection capability of embedded devices. This is true though future protocol standards and legal regulations are still needed in parallel.

### *E. RFID Specific Mitigations:*

For attacks on RFID tags, [13] suggests personal firewalls to examine all readers' requests to read tags, along with the use of cryptography, though full encryption is difficult with IoT resource constraints. Hash-based schemes are more widely used, where a RFID reader gets a hashed key from a locked RFID tag which it sends to a database. The database returns a key to the reader which it uses to unlock the tag.

### *F. Reducing Risk Through Legislation:*

Of the resources surveyed, Verizon [23] are one of the few to mention changing the law as a form of mitigation, discussing data protection laws and the trade-off between security and convenience. Without legislation, manufacturers can't be compelled to include security [20], and IoT will have to comply with European regulatory frameworks. For example, it is expected 80% of households will have energy meters by 2020 [24].

## VIII. Conclusions & Future Work

One could go so far as to say the vulnerabilities outweigh counter measures. Mitigations based on IP are not enough due to device constraints and, as it the present point in time, a lack of standards. A lot has been written (and repeated) with regard to protocols and channel based security solutions.

Therefore, plenty of research opportunities exist elsewhere, like in energy saving cryptography techniques that are lightweight enough for IoT, the use of IDS in IoT and how to do more with the constrained resources of devices – recall also that processing power doubles every two years according to Moore's Law, so some mitigations that exist now could just be a stopgap until the device resources catch up. In addition, none of the surveyed papers covered the issue of mobility in IoT. The rise in popularity of wearables poses a complex issue of handling devices regularly leaving one NoT and joining another.

IoT is set to impact society significantly, and with attackers already exploiting the early adoption of IoT in a myriad of ways, a new conclusion can be drawn that IoT will become the most vulnerable area of cyber security, with the race already underway to protect both legacy and future devices through technology and robust legislation.

## Acknowledgment

This paper was supported by the Centre for Secure Information Technologies (CSIT), at the Queen's University of Belfast.

## REFERENCES

[1] S. Nalbandian, "A survey on Internet of Things: applications and challenges", Second International Congress on Technology, Communication and Knowledge (ICTCK 2015), Mashhad Branch, Islamic Azad University, Mashhad, Iran, November 2015

[2] CISCO, "The Internet of Things Reference Model", White Paper, June 2014

[3] Hewlett Packard, "Internet of things research study", 2015

[4] M. Leo, F. Battisti, M. Carli, A. Neri, "A federated architecture approach for Internet of Things security", November 2014

[5] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", 2003

[6] W. Shang, Y. Yu, R. Droms, L. Zhang, "Challenges in IoT Networking via TCP/IP Architecture", NDN Technical Report NDN-0038, February 2016

[7] O. Garcia-Morchon et al., "Security Considerations in the IP-based Internet of Things", CoRE Internet-Draft, September 2013

[8] H. Kim, A. Wasicek, B. Mehne, E. Lee, "A Secure Network Architecture for the Internet of Things Based on Local Authorization Entities", 2016 IEEE 4th International Conference on Future Internet of Things and Cloud

[9] R. Roman, J. Lopez, "Integrating Wireless Sensor Networks and the Internet: A Security Analysis", Internet Research, vol. 19, p246-259, 2009

[10] X. Xingmei, Z. Jing, W. He, "Research on the Basic Characteristics, the Key Technologies, the Network Architecture and Security Problems of the Internet of Things", 3rd International Conference on Computer Science and Network Technology, 2013

[11] D. Zegzhda, T. Stepanova, "Achieving Internet of Thing Security via Providing Topological Sustainability", Science and Information Conference, July 2015

[12] R. Mahoud, T. Yousuf, F. Aloul, I. Zualkerman, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures", The 10th International Conference for Internet Technology and Secured Transactions, 2015

[13] A. Mohsen, N. Jha, "A Comprehensive Study of Security of Internet-of-Things", 2016

[14] S. Elbouanani, M. El Kiram, O. Achbarou, "Introduction To The Internet Of Things Security", 11th International Conference on Information Assurance and Security (IAS), 2015

[15] S. Keoh, S. Kumar, H. Tschofenig, "Securing the Internet of Things: A Standardization Perspective", IEEE Internet Of Things Journal, Vol. 1, No. 3. June 2014

[16] I. Andrea, C. Chrysostomou, G. Hadjichristofi, "Internet of Things: Security Vulnerabilities and Challenges", 3rd IEEE ISSC 2015 International Workshop on Smart City and Ubiquitous Computing Applications

[17] OWASP Internet of Things Project, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_internet_of_things_Top_10_for_2014, accessed 19th October 2016

[18] A. Wood, L. Fang, J. Stankovic, T. He, "SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks", October 2006

[19] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", 2012

[20] C. Tankard, "The security issues of the Internet of Things", Computer Fraud & Security, September 2015

[21] S. Raza, L. Wallgren, T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", Ad Hoc Networks 11 pg 2661-2674, 2013

[22] A. Gendreau, M. Moorman, "Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things", IEEE 4th International Conference on Future Internet of Things and Cloud, 2016

[23] Verizon, "State of the Market: The Internet of Things 2015", 2015

[24] M. Weber, M. Boban, "Security challenges of the Internet of Things", MIPRO 2016 Opatija, Croatia, May-June 2016